Amendments to the Specification:

Please amend paragraph beginning on page 1, line 7 as follows:

The present invention generally relates to **the** field of data processing and more particularly to a method and implementation for secured or authenticated access to a storage area network, particularly, a Fibre Channel compliant storage area network.

Please amend paragraph beginning on page 2, line 6 as follows:

Unfortunately, the openness that is at least partially responsible for the increasing prevalence of Fibre Channel storage area networks, creates a potentially significant security issue for a tremendous number of large (as well as small) and highly valued databases. As an open standard, the Fibre Channel network is susceptible to many of the same security concerns as the Internet. A malicious hacker who was able to gain control of a host bus adapter connected to a Fibre Channel switch may be able to alter, delete, or otherwise damage data across the entire SAN. An unauthorized user who gains access to a Fibre Channel fabric attached element can ~~{comprise}~~ **compromise** a Fibre Channel switch in at least three ways. First, the user may write software to use the existing Fibre Channel device interface to ~~{comprise}~~ **compromise** the fabric operating environment. Second, the user could install device level drivers that try to compromise the fabric operating environment at the Fibre Channel physical and signaling interface (FC-PH) level. Third, the user could install a doctored host bus adapter that has hardware or micro-code that tries to exploit the fabric operating environment at the FC-PH level. Therefore, it would be highly desirable to implement a secure and cost effective mechanism for assuring the integrity of transactions that occur on a SAN network.

Please amend paragraph beginning on page 4, line 26 as follows:

The depicted embodiment of SAN 105 includes a set of nodes 120 that are interconnected through a Fibre Channel fabric 101. The nodes 120 of network 100 may include any of a variety of devices or systems including, as shown in FIG 1A, one or more data processing systems (computers) 102, tape subsystems 104, RAID devices 106, disk subsystems 108, Fibre Channel arbitrated loops (FCAL) 110, and other suitable data storage and data processing devices. One or more nodes 120 of network 100 may be connected to an external network denoted by reference numeral 103. The external network 103 may **be** a local area network (LAN) or an IP supported network such as the Internet. Typically, Fibre Channel fabric 101 includes one or more interconnected Fibre Channel switches 130, each of which includes a set of Fibre Channel ports 140. Each port 140 typically includes a connector, a transmitter, a receiver, and supporting logic for one end of a Fibre Channel link and may further include a controller. Ports 140 act as repeaters for all other ports 140 in fabric 101. Fibre channel ports are described according to their topology type. An F port denotes a switch port (such as are shown in FIG 1B), an L or NL port denotes an Arbitrated-Loop link (not shown in FIG 1B), and an FL port denotes an Arbitrated-Loop to Switch connection port. The ports 140 communicate in a standardized manner that is independent of their topology type, allowing Fibre Channel to support inter-topology communication.

Please amend paragraph beginning on page 6, line 30 as follows:

Referring now to FIGs 3 and 4, block diagrams illustrating hardware and software components respectively that are used in conjunction with an authenticated Fibre Channel fabric login sequence as described herein are presented. In the depicted embodiment, a node 120 and a switch 130 form a Fibre Channel connection. More specifically, a HBA 210 on node 120 is connected to a switch port 140 of switch **130** via a copper or fiber optic cable 303. The node 120 includes a non-volatile memory device 302 and a system memory 206 that are accessible to host bus adapter 210 via one or more busses. Similarly on the switch side of the connection, switch 130 includes a non-volatile storage device 304 and a switch memory 306 that are accessible to switch port 140.

Please amend paragraph beginning on page 7, line 29 as follows:

The encryption keys and password tables that are generated by key server 408 should be transferred to the various ~~{host}~~ **hosts** via an entrusted mechanism. In one embodiment, the keys and passwords tables could be generated and stored on a portable storage device such as a floppy diskette and manually installed on each host by an administrator or other privileged and entrusted user. In another embodiment, the keys and passwords tables may be delivered to each host 120 over an external network via a trusted, and preferably ~~{encrypted, link}~~ **encrypted link**. A secure IP link, for example, might be used to distribute the various keys and password tables to each node 120. This distribution method might itself be performed with an application requiring secure access such as a passworded application.

Please amend paragraph beginning on page 7, line 29 as follows:

Referring now to FIG 5, a flow diagram of one embodiment of a Fibre Channel fabric authentication mechanism and method 500 as contemplated is presented. The method 500 may be implemented as a computer program product (software) in which a set of processor executable instructions for authenticating access to SAN 105 are stored on a computer readable medium such as a floppy diskette, CD ROM, hard drive, tape storage, a non-volatile memory device such as a PROM, EEPROM, or flash device, or in a system memory or cache memory associated with one or more processors. Various portions of the software may be executed by a processor on a node 120 while others may be executed by a processor in a switch 130 of network 100. Similarly, various portions of a software implementation of method 500 may comprise portions of switch's SAN software interface 416 or the node's software interface 406. In one embodiment (as depicted in FIG 4) the authentication is performed by software interfaces 406 and 416 on either side of the link. The host software interface monitors the host for events that trigger portions of the authentication mechanism. If, for example, a power up or software reset is ~~{detect}~~ **detected** (block 502) the host software interface 406 will read (block 504) an identifying number of the host device (such as the serial number). From the serial number, software interface 406 can generate a bind code and compare (block 506) the generated bind code against that was stored when the bind codes were originally generated (such as when the host 120 was

initially installed). If the generated bind code and the stored bind code do not match, the software interface is disabled (block 508) and the system administrator is notified. The bind code may be further enhanced by incorporating additional information in the code. A time stamp and date stamp may be used when the bind code is initially generated. If the time stamp and date stamp detected during a subsequent power on or software reset are not chronologically greater than (i.e., after) the originally detected date and time stamps, the software may abort. This hardware/software binding prevents an unauthorized user from physically swapping an unauthorized HBA for an authorized HBA as a means of gaining unauthorized access to SAN 105. Similarly, the binding codes prevents an unauthorized user from installing an unauthorized version of software interface 406 in an attempt to access SAN 105. Thus, the described binding mechanism provides an additional level of security for SAN 105. When a power up sequence or software reset occurs, the unauthorized HBA and/or software interface will be unable to retrieve the required binding codes thereby preventing access to the key generation application, without which the user will be unable to access SAN 105.

Please amend paragraph beginning on page 9, line 18 as follows:

Assuming that a power up sequence has been performed successfully and the bind code of each hard device is verified (and assuming no software reset events occur), software interface 406 will monitor for an event that triggers an authenticated fabric login sequence according to the present invention. Preferably, the authenticated login sequence is launched ~~{each time}~~ each time there is a normal switch login and each time there is an abnormal switch event (login or logout). Upon the occurrence of such an event, software interface 406 requests (block 510) a login to switch 130. In response, a software interface 416 on switch 130 generates a random hash (block 512) into password table 412. A password is then retrieved from the password table 412 based upon the random hash. This password, itself, represents a hash into password table 412. Software interface 416 determines from table 412 a response value that corresponds to the hash represented by the retrieved password. Software interface 416 stores (block 516) this response locally and encrypts (block 518) the corresponding password according to the encryption key that is stored in a secret and preferably non-volatile location on switch 130. The encrypted password is then sent (block 520) to host 120 wherein software interface 406 decrypts the password (block 522) based upon its locally stored copy of the encryption key (which is the same as the encryption key stored in switch 130) and uses the decrypted password to hash into host password table 402. The location of host password table 402, like the location of switch password table 412 is known only to the corresponding software interface. Upon retrieving the password from its password table 402, software interface 406 encrypts (block 524) the response according to its locally stored encryption key sends the response back to switch 130. Upon receiving the encrypted response from host 120, software interface 416 decrypts the response using the encryption key and compares the received response with the value of the response stored in block 516. If the response matches, software interface 416 permits (block 530) the login to Fibre Channel fabric 101 and informs the requestor of successful completion. If the response does not match, the fabric login is denied (block 528) and the requestor is prevented from accessing fabric 101.